Los Alamos

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

OS-DO-82-265

August 4, 1982

STAT [redacted]

Dear Bob:

In response to your request for a "tiger team" approach to a security analysis of the system, we would like to suggest the following. The first activity is the "tiger team" which we estimate to be about 20 man-weeks total effort, the cost of travel for two people to Washington D.C. for three weeks, plus the cost of manuals for the system. The "tiger team" effort will include 1) attempts to break the system security features, 2) defeat internal file protection, 3) find software problems, 4) find hardware problems. We assume that the system will be used in a friendly environment and that we will not be allowed to plan any physical damage to the hardware. The total cost of this activitiy will be approximately $50K.

While this approach is not as good as a formal security analysis, it will allow the review of the system for possible problem areas. A formal security analysis would allow the review of system level documentation and source code. As you know, the "tiger team" approach is inherently subject to omissions and can lead to serious wrong conclusions.

We propose, as an option, to extend our activity at a low level of effort for a longer period of time possibly with FY-83 funds. This option would have the advantage of a longer review of the system during actual usage. Periodic reports would be made plus detailed reports whenever new problems were found. The main cost of this option would be the cost of a fraction of a system plus some cost for man power. The real advantage is that there will be a better understanding of the system since more time will have been spent with it.

SYSTEM SECURITY

The operating system is the main area of concern because it has the responsibility to protect all the data and programs in the system. In this system, it is the only place which the vendor claims to provide system security. This security is based on allowing only authorized users (user IDs) to log-on the system. The advertised security features provide the system manager with the ability and the responsibility to create levels of system access based on the requirements of each user. The user is assigned to a designated class, given a USER ID, and optionally given a PASSWORD. Methods which will be investigated to circumvent the system security will include; 1) tests of the log-on procedure, 2) tests of the system's enforcement of class assignments, 3) tests of the system's file password control.

INTERNAL FILE PROTECTION

Another important area for system security is the protection of files from system's and users' programs. The system allows CP/M (and in theory any CP/M user software) and BASIC programs to be run from any workstation. While this is a nice feature, it could lead to the possibility of writing programs which could change the passwords of files and then allow other system utilities to delete, modify, copy, or archive files of other users. Methods which will be used to check for this problem will include 1) induced input errors to system utilities, 2) writing BASIC programs which try to read other users' files, 3) using CP/M features to modify or change other users' files.

SOFTWARE PROBLEMS

Software problems can be divided into two general classes. The first is a software "bug" and the second is a design error. The software "bug" is found by luck, if it is found at all in a short period of time. The design error is generally found by review of source code and documentation. Software problems can and often do lead to operational problems which cause the system manager or other users to relax their guard and take short cuts which reduces the effectiveness of the system security features. Methods which will be used to try to find software problems include; 1) review of user documentation, 2) test of inputs to some of the system utilities, 3) review of user interfaces (CP/M, BASIC, and vendor supplied programs).

HARDWARE PROBLEMS

Hardware problems, like software problems, can be divided into two general classes. The first is a component which fails and the second is a design error. From the security point of view design errors are generally in the form of omissions of hardware which would protect parts of memory, limit access to I/O devices, limit some automatic system actions, or record some actions taken by the system or users. Component errors are hard to predict but if found can often be used advantageously. Methods which would be used to find hardware problems include; 1) induced power problems, and 2) induced communication problems. We would also investigate approaches to mitigating the known power-on problem.

Sincerely,

Dave

D. Bailey

DB:sp

xc: M. Heinberg, OS-2, MS-E508
R. Stutz, ENG-8, MS-M706
E. Tucker, IT-3, MS-B231
CRMO (2), MS-A150
OS-DO File